NIH Clinical Center CIO Newsletter

March 2008

27th Edition

This is the twenty-seventh edition of a monthly broadcast email to the CRIS user community about CRIS capabilities and issues. In addition to the text version in this email, I've attached a PDF version that can be printed. I look forward to receiving your comments or suggestions at CIOnewsletter@cc.nih.gov

Topics of the Month

- CIO Remarks
- Sharing CRIS Codes
- Information System Security Department
- NIH Information Technology General Rules of Behavior
- Security Awareness Training Requirements
- HHS Information Security Program
- Laptop Security
- New DTM Blood Products Labeling
- CITRIX Update
- New Urinalysis Test
- User Training
- Pharmacy Project Update
- FDCC Initiative for the Clinical Center

CIO Remarks

As an undergraduate computer science student 20 years ago I remember a professor stating "that with technology comes great responsibility". This was a variation of "with great power comes great responsibility" and "with money comes responsibility". Responsibilities of technology are based on the systems themselves as well as the ease of accessibility of data. Three important responsibilities for both users of technology and those who support technology are integrity of the data/system; safety and protection of the data within the system; and availability, maintenance and continuous system improvement.

Within DCRI there are many people, in many different roles, whose charge it is to meet these three main responsibilities for CRIS. CRIS Training and CRIS Configuration and Development support data/system integrity. CRIS Support, the CC Privacy Officer and the CC Information Systems Security Officer monitor and protect the data within CRIS. And Desktop Support, Systems Administration, Network Administration, Systems Monitoring, and Project Management assure that the system is available and maintained. Everyone works to continuously improve the system. The specific responsibilities of the CC CIO were detailed in http://cris.cc.nih.gov/cionews/pdfs/NIH_CC_CIO_Newsletter_August_2007.pdf

However, I think it important to note, these responsibilities not only apply to those who maintain CRIS, but also to every CRIS user. Listed below are some examples of responsibilities we all have as CRIS users

- Maintain the integrity of CRIS and the data therein: select the appropriate protocol when placing a medical order; complete order forms and documentation accurately; assign orders to the correct physician; sign orders when appropriate; document medication administration tasks, etc.
- Safeguard and protect the data within the CRIS: do not share account identification and passwords; log out promptly to help prevent unauthorized access; file clinical printouts in the medical record when appropriate; shred printouts containing any personally identifiable information; understand and comply with NIH security and system confidentiality policies; report breaches of security or patient confidentiality, etc.
- Continue to maintain and to improve the CRIS: report any issues, problems or suggestions for improvement through the CRIS Support (301-496-8400). CRIS is **YOUR** system, please use **YOUR** voice to identify improvement opportunities. Feel free to e-mail me at CIONewsletter@cc.nih.gov with any suggestions or comments.

Sharing CRIS Codes

The security of your Clinical Research Information System (CRIS) code is a very serious matter. The Medical Executive Committee mandates serious sanctions if practitioners are identified as having shared their codes. These sanctions involve (at a minimum) suspension of your CRIS code and CRIS retraining. In addition to these mandatory penalties, the Medical Executive Committee may impose additional sanctions, including suspension of clinical privileges or termination of employment. Sharing your code is equivalent to allowing someone else to use your signature, with the substantial personal and institutional liabilities that behavior might

entail. Maintaining the security of your code protects our institution, our staff, and our patients. These codes simply must not be shared. Prior to receiving a CRIS code, every user must sign the NIH Clinical Center Confidentiality Agreement which details both general confidentiality/privacy guidelines as well as computer access confidentiality measures. If you need a copy of the Confidentiality Agreement, please contact CRIS Support at 301-496-8400.

The CRIS Password Security Policy (Medical Administrative Series policy M05-4) outlines the requirements for password security as well as the penalties for violating the policy. The complete policy may be viewed at: http://internal.cc.nih.gov/policies/PDF/M05-4.pdf

For those of you who need a code to access CRIS, you must first take CRIS training which is available twice a week, typically every Monday and Thursday. To obtain a CRIS code after training has been completed, a valid NIH ID badge is required.

Information System Security Department

The Clinical Center (CC) Information System Security Department is responsible for the coordination, implementation, and enforcement of Government-required information security policies that affect the CC. The department is led by John Franco the Information System Security Officer (ISSO) and Boniface Lansiquot is the Associate Information System Security Officer. Some of the Government-required information security policies that affect the CC are the Federal Information Security Management Act (FISMA), and the E-Government Act. Some of the responsibilities of the department are, but not limited to:

1. Evaluate new or existing systems to assure compliance with applicable laws and regulations.
2. Provide guidance to CC employees on computer security issues related to the acquisition, utilization, and disposal of computer hardware and software.
3. Create and/or distribute written computer security policies and procedures that enable the CC to achieve its mission.
4. Ensure that all CC employees are exposed to computer security awareness and training.
5. Receive, monitor and investigate allegations of improper/illegal activities by employees who may have violated privacy/confidentiality, security policies, regulations or other requirements thus jeopardizing the security of CC computer systems.

The Information System Security Department works to ensure the Confidentiality, Integrity, and Availability of all Clinical Center computer systems. To help accomplish this task, the security department will be working with the CC acquisition teams to achieve a new NIH initiative focused on ensuring that FISMA and other government information security requirements are in all necessary CC computer hardware and software acquisitions.

The Information System Security Department is available to answer or recommend solutions to computer security related questions or concerns. John Franco has been a CC employee for more than 20 years and can be reached via NIH e-mail or at (301) 285-9412. Boniface Lansiquot can be reach via NIH e-mail or at (301) 435-7924.

NIH Information Technology General Rules of Behavior

Please refer to http://irm.cit.nih.gov/public/nihitrob.html for the complete General Rules of Behavior. Appropriate use of the internet and E-mail are listed below.

- Refer to and abide by the Guidelines for Appropriate Use of the World Wide Web by NIH Employees at http://irm.cit.nih.gov/policy/guideli2.html.
- Refer to and abide by the NIH Web Page Privacy Policy at http://www3.od.nih.gov/oma/manualchapters/management/2805/.
- Use the Internet for business purposes only when on official government time or in accordance with the NIH Personal Use policy located at http://www3.od.nih.gov/oma/manualchapters/management/2806/.
- Be aware when navigating through the Internet; you may be moving from an area of controlled access into an area of unknown security controls.
- Report any security incidents to the appropriate officials.
- Do NOT send sensitive information via e-mail or fax, unless encrypted.
- Refer to http://oma.od.nih.gov/ms/records/rmanagement.html for the latest guidance on records requirements for official e-mail records and facsimile documents, or contact your IC Records Management Officer.
- Protect copyrighted software and information in accordance with the conditions under which it is provided.
- All Contractor staff who have access to and use NIH e-mail must set up an AutoSignature or electronic business card (v-card) on their computer and/or personal digital assistant (PDA) to visibly identify themselves as a contractor on all outgoing e-mail messages, including those that are sent in reply and on messages that are forwarded to another user. For more information, see "New Requirements for NIH Contractor" Designations in Email located at http://irm.cit.nih.gov/policy/contractors.html
- Ensure Sensitive and Privacy Act information is not transmitted using personal e-mail accounts (HHS Information Security Program Policy).

Security Awareness Training Requirements

Please be aware that because we are now in a new fiscal year, the required Security Awareness Training (http://irtsectraining.nih.gov/) has been updated to include the FY '08 Refresher component. You may check your status when viewing your student record. As with previous years, those taking the initial full security awareness course after October 1st, will automatically receive credit for the FY08 Refresher (i.e., if they previously took the course, and just repeated it, they do NOT receive credit for the

Refresher---it's just the first time). All NIH employees and contractors are required to complete the refresher by June 30, 2008. Remember – you'll have to review and acknowledge that you have read the NIH Rules of Behavior as part of this annual training.

HHS Information Security Program

The HHS Information Security Program identifies Employee Responsibilities by role including Supervisors and Employees. Listed below are sections that discuss the responsibilities of Supervisors and Users and Employees. For the complete information please refer to http://intranet.hhs.gov/infosec/docs/policies_guides/ISPP/isp_toc.htm

Supervisors are responsible for:

- Ensuring compliance with information security policies by all personnel under their direction and providing the personnel, financial, and physical resources required to protect information resources appropriately;
- Ensuring that their direct reports complete all required IT security training within the mandated time frame;
- Notifying the appropriate OPDIV ISSO immediately of the unfriendly departure or separation of a Department or contractor; if the ISSO is not available, then they should contact the appropriate OPDIV CISO immediately; and
- Pursuing disciplinary or adverse actions against personnel and contractors who violate the *HHS Information Security Program Policy, HHS Information Security Program Rules of Behavior*, and system-specific rules of behavior. 2.2.4.12 Users and Employee

The Department's users and employees are responsible for:

- Complying with the Department's policies, standards, and procedures;
- Being aware they are not acting in an official capacity when using Departmental IT resources for non-governmental purposes;
- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data;
- Reporting any suspected or actual computer incidents immediately to the OPDIV IRT;
- Seeking guidance from their supervisors when in doubt about implementing this policy document;
- Ensuring that all media containing Departmental data is appropriately marked and labeled to indicate the sensitivity of the data;

- Refraining from loading unapproved software on Departmental systems or networks;
- Ensuring that sensitive data is not stored on laptop computers or other portable devices unless the data is secured using encryption standards that are commensurate with the sensitive level of the data;
- Reading, acknowledging, signing, and complying with the HHS Information Security Program Rules of Behavior and OPDIV- and system-specific rules of behavior before gaining access to the Department's systems and networks;
- Implementing specified security safeguards to prevent fraud, waste, or abuse of the systems, networks, and data they are authorized to use;
- Conforming to security policies and procedures that minimize the risk to the Department's systems, networks, and data from malicious software and intrusions;
- Agreeing not to disable, remove, install with intent to bypass, or otherwise alter security settings or administrative settings designed to protect Departmental IT resources; and
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving their workstation.

Laptop Security

All NIH laptops should be encrypted using the PointSec encryption software, unless they are covered under a waiver signed by the NIH Chief Information Security Officer (CISO) and the HHS CISO.

(1)All HHS laptop computers in your IC are secured using a Federal Information Processing Standard (FIPS) 140-2 compliant whole-disk encryption solution, or are covered by a waiver approved by the NIH and HHS CISOs.

(2) All mobile devices and portable media in your IC that contain sensitive
NIH or HHS agency data are encrypted using a FIPS 140-2 compliant product.

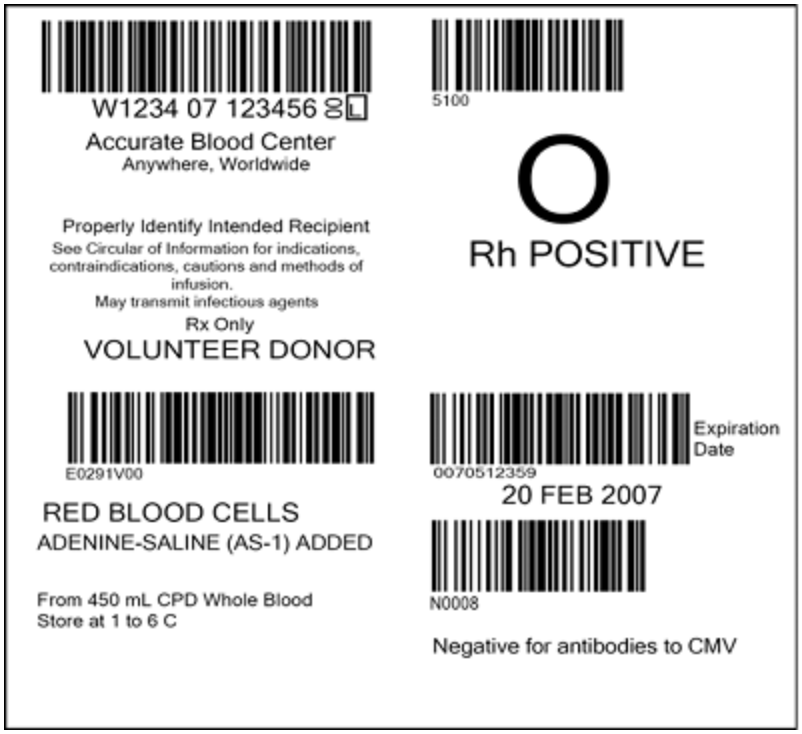
Please note that for the time being Macintosh computers are covered by a waiver, but the waiver stipulates that no unencrypted sensitive information or personally identifiable information (PII) can be stored on those devices. We are working with HHS on a refinement of this waiver to allow the use of FileVault file-based encryption software under certain conditions.

Thank you for your assistance in ensuring the integrity and security of NIH
data. We will keep you informed if there are any further developments regarding Encryption for Macintosh Computers.

New DTM Blood Products Labeling

The Department of Transfusion Medicine will be implementing a new labeling format for blood components beginning April 28, 2008. The change utilizes a bar code symbology called *ISBT 128* and is mandated by the AABB to be implemented on or before May 1, 2008 by all association members. The labeling format was designed by the International Society for Blood Transfusion (ISBT) and is maintained by the International Council for Commonality in Blood Banking Automation, Inc. (ICCBBA). Its purpose is to provide a global standard for the identification, labeling and information processing of human blood, tissue and organ products across international borders and disparate health care systems. *ISBT 128* provides for unique identification of any donation worldwide. It does this by using a 13 character identifier built up from three elements, the first identifying the collection facility, the second the year, and the third a sequence number for the donation. The appearance of the blood label will change to an all black and white format laid out in quadrants each displayed in both bar code and eye readable formats. The quadrants display the unique donation number, ABO Rh group and type, product code and expiration date. Look for more information in the April edition of CC Nursing Quick Updates. For additional information please contact Sherry Sheldon (301) 451-8654 or Karen Byrne (301) 451-8645.

Below is a generic example of the new ISBT 128 label.


W1234 07 123456
Accurate Blood Center
Anywhere, Worldwide
Properly Identify Intended Recipient
See Circular of Information for indications, contraindications, cautions and methods of infusion.
May transmit infectious agents
Rx Only
VOLUNTEER DONOR
E0291V00
RED BLOOD CELLS
ADENINE-SALINE (AS-1) ADDED
From 450 mL CPD Whole Blood
Store at 1 to 6 C
5100
O
Rh POSITIVE
0070512359
Expiration Date
20 FEB 2007
N0008
Negative for antibodies to CMV

CITRIX Update

The Department of Clinical Research Informatics (DCRI) is continuing to upgrade the CC Citrix Farm and move applications to the new web-based interface (https://cccasper.cc.nih.gov).

The following applications were migrated/launched in early March:

- Cerner (Radiology)
- Crimson (NIAID application)

Upcoming application migrations/implementations in March include:

- Published Desktop
- Hospital Services

The Citrix Published Desktop provides access to such applications as Microsoft Office (Word, Excel, Outlook, Visio, Project, PowerPoint, etc.), Admissions, BBD, Building Services, Institute Reports, NCI Census, ORS, Ansos, etc. After these migrations, all the major applications will have been moved to the upgraded Citrix Farm. Six to eight weeks after March 31, the DCRI Citrix team will retire the old Citrix Farm (e.g. "Casper" web site) and you will access all CC Citrix-provided applications via the new "CCCasper" web site.

Please contact Judy Wight at wightj@cc.nih.gov or 301-443-3477 if you have any questions.

New Urinalysis Test

NIDDK currently offers a manually performed urinalysis study in conjunction with its consults. This CLIA-approved study is now available as an order in CRIS, known as Urinalysis (Nephrology Consult), and requires prior approval from a Nephrology Consultant. The order will generate a label for the specimen, which is to be delivered to CRC-5SW Day Hospital, Rm. 5-5624 (not DLM). Results from the study will be available on the Results Tab in CRIS. Please call 301-496-8820 with any questions.

User Training

Coming Mid-Spring 2008, the Department of Clinical Research Informatics (DCRI) will proudly unveil a new era in CRIS Prescriber Training: **Online Availability**. The changes to training were made based on requests from members of the NIH Prescriber community.

The new training format will offer the following advantages:

- 24 hour access to course material
- Remote access (outside of DCRI Classroom and/or NIH campus)
- Optional completion prior to arrival at NIH
- Enhanced online tutorials

When this new program is initiated, incoming prescribers will receive detailed instructions *via their email* of record following the submission of their credentialing packet to the Office of Credentialing Services. Subsequently, online CRIS training can begin at any time. It is recommended that prescribers fulfill their CRIS training requirements as early as possible, preferably prior to entry on duty (EOD).

NOTE: Institutes and Departments will be expected to provide workstation space to access CRIS online training for those new prescribers who have not concluded CRIS coursework prior to EOD. **Therefore, we encourage that space/location and logistics planning for new employee CRIS training begin at the Institute/Department level as soon as possible.**

In the upcoming weeks, program coordinators and key stakeholders will be receiving additional information to assist in planning for the CRIS training needs of new medical staff. We are excited about this new training format and hope that you will be pleased with it as well.

Please feel free to contact the CRIS Training Team at (301) 496-8400 if you have any questions or concerns.

Pharmacy Project Update

DCRI and Pharmacy are implementing a pharmacy information system called Sunrise Medication Manager (SMM), which is integrated within CRIS. This pharmacy system will allow us in the future to use the full capability of automated dispensing cabinets (such as Pyxis) located on nursing units, and also enable us to interface with bedside barcode scanning systems used during medication administration. These systems will not only increase the safety of the medication use process, but also decrease the time for the patient to receive first doses of newly ordered medication.

Prescribers should notice little or no change in the CRIS medication ordering process, though the order form layouts will be more standardized. Implementation of the first phase of SMM (Oral Medications) is scheduled for May 31st, June 1st and 2nd. The second phase implementation in mid-July will involve intravenous medications. Future plans also include

procurement of a robotic filling system for take-home prescriptions, which will decrease waiting time in the Outpatient Pharmacy.

Reminder This is a huge project and will require the efforts of the entire DCRI staff to complete it over the next few months (April through the end of May). As a result our ability to handle requests for order sets and non-emergency work in CRIS will be significantly reduced. Projects of any type that are not directly related to the pharmacy computer system project will be evaluated on a case-by-case basis during this time.

FDCC Initiative for the Clinical Center

The Clinical Center's IT support staff has been working to implement an important Office of Management and Budget (OMB) directive to standardize the configuration of government furnished Windows XP and Vista personal computers. As we noted last month, the primary intent of this change is to strengthen Federal IT security by reducing opportunities for hackers to access and exploit government computer systems. The new configuration is referred to as the Federal Desktop Core Configuration (FDCC) and consists of standardizing approximately 300 configuration settings on each computer.

- The team is working to contact departments regarding the dates when these settings will be applied.
- The team is also requesting assistance to test applications with the FDCC settings that are unique to each department. This will be done prior to implementing the settings to the entire department.

As of March 26, 2008, the team has implemented these settings on 25% of the Clinical Center workstations and the project remains on schedule.

Note: New Office 2007 upgrades and new Vista systems will not be deployed until after the completion of this project to avoid any conflicts.